AML / CFT Policy

Version 1.01 / July 26, 2023

Company Policy

1.1 Bitplay Global B.V. (the "Company") strictly prohibits and actively prevents money laundering and any activities that facilitate money laundering or the financing of terrorist or criminal activities. The Company is committed to complying with all relevant requirements under the legislations in force in the European Union member jurisdictions where it operates, including Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for money laundering and terrorist financing, as well as the forthcoming Fourth Directive on Money laundering.

1.2 Money laundering entails acts aimed at concealing or disguising the true origins of proceeds obtained through criminal means, making them appear legitimate.

1.3 Terrorist financing may not involve proceeds of criminal conduct but instead attempts to conceal the origin or intended use of funds, which could be for criminal purposes. Notably, legitimate sources of funds distinguish terrorist financiers from traditional criminal organizations.

1.4 While the motivations differ between money launderers and terrorist financiers, the methods employed to fund terrorist operations may resemble those used by criminals to launder funds. Funding terrorist attacks may not require large sums, and transactions associated with it may not be complex.

The objective of the Policy

2.1 The Company is fully committed to maintaining constant vigilance to prevent money laundering and combat the financing of terrorism, aiming to minimize and manage risks, including reputational, legal, and regulatory risks. It also acknowledges its social responsibility to prevent serious crime and ensure that its systems are not abused for such purposes.

2.2 The Company will actively monitor national and international developments related to anti-money laundering and counter-terrorist financing initiatives. It is dedicated to safeguarding its organization, operations, and reputation from the threats of money laundering, terrorist financing, and other criminal activities.

2.3 The Company's policies, procedures, and internal controls are designed to ensure compliance with all applicable laws, rules, directives, and regulations about its operations. These policies will be regularly reviewed and updated to ensure their effectiveness.

Player Identification Program

3.1 The Company will take reasonable steps to verify the identity of all individuals (hereinafter "Players") intending to use its services. The registration process for Players, as defined in the General Terms and Conditions of the Company, includes a due diligence process that must be completed before opening a user account.

3.2 The Company will maintain a secure online list of all registered Players, ensuring that information and documents are retained in accordance with applicable data protection obligations.

3.3 When opening an account, the Company will collect certain minimum identification information from each Player. Anonymous accounts or accounts under fictitious names, where the true beneficial owner is unknown, will not be accepted. The required information will include, at a minimum:

- Player's date of birth (confirming the player is over eighteen (18) years old).
- Player's first and last name.
- Player's place of residence.
- Player's valid email address.

3.4 When there is a perceived risk or uncertainty about the information provided, or before any payment exceeding 3000 USD per occasion or when payments to the account exceed 3000 USD, the Company will request verification documents from the Player. These documents may include, to the extent permitted under relevant data protection regulations:

- a driver's license;
- an identity card issued by the local government;
- a travel document or passport;
- proof of address (utility bill)

3.5 The Company may complement documentary evidence with other means, such as:

- Independently verifying the Player's identity by comparing the provided information with data obtained from reporting agencies, public databases, or other reliable sources.
- Checking references with financial institutions.
- Obtaining a financial statement.

3.6 Relevant Players will be informed that the Company may seek identification information to verify their identity. The Company will conduct monthly comparisons of Player identification

information with government or international-provided lists of suspected terrorists or sanctioned individuals, such as those provided by the European Union or FATF.

3.7 If a Player appears on a list of suspected terrorists or sanctioned individuals, the Company will take immediate steps to freeze or close the Player's account.

3.8 If any material or personal information of a Player changes, the Company will request verification documents.

Continuous Transaction Due Diligence

4.1 The Company will closely monitor account activity, particularly transactions that are more complex, large, or likely related to money laundering or terrorist financing.

4.2 Parameters indicating possible money laundering or terrorist financing include, but are not limited to:

- Transactions from high-risk geographic locations without apparent justification.
- Numerous small, incoming money transfers or deposits followed by immediate withdrawals.
- Unexplained, repetitive, unusually large, or patterned deposit activity without a specific purpose.

4.3 The Company will not accept cash or non-electronic payments from Players. Funds may be received only through approved crypto payment methods.

4.4 Payments of winnings or refunds will be transferred back to the same route from which the funds originated whenever possible.

4.5 Transfers of funds between Players' accounts will be prohibited.

4.6 If the Company utilizes a third party to process and record payments to and from Player accounts, the service provider must have transaction monitoring systems in line with these provisions and applicable legislation.

4.7 Financial transaction records will be maintained in accordance with data protection and retention requirements in the applicable jurisdiction of Curaçao.